AMENDMENTS TO THE CLAIMS

1. (Currently amended) A method of securing communication of configuration data between a field programmable gate array (FPGA) and an external storage device, the method comprising:

generating a fingerprint within the FPGA, the fingerprint representing an inherent manufacturing process characteristic unique to the FPGA, wherein generating the fingerprint includes measuring propagation delays for a plurality of circuit elements on the FPGA and combining the propagation delays to generate the fingerprint;

transmitting encrypted configuration data from the storage device to the FPGA; and

decrypting the encrypted configuration data in the FPGA using the fingerprint as a decryption key to extract the configuration data.

2. (Original) The method of Claim 1, further comprising:

configuring the FPGA using the configuration data.

3. (Original) The method of Claim 2, further comprising:

transmitting the fingerprint from the FPGA to an encryption circuit;

encrypting the configuration data using the fingerprint as an encryption key; and

storing the encrypted configuration data in the storage device.

4. (Original) The method of Claim 1, wherein the fingerprint is generated during power-up of the FPGA.

Claim 5. (Cancelled)

6. (Currently Amended) The method of Claim 1 [[5]], wherein generating the fingerprint further comprises:

counting the number of oscillations of an oscillator on the FPGA during a predetermined time interval.

7. (Original) The method of Claim 6, wherein the oscillator comprises a configurable logic block of the FPGA.

8. (Currently Amended) The method of Claim 1 [[5]], wherein generating the fingerprint further comprises:

counting the number of oscillations of a first oscillator on the FPGA during a predetermined time interval;

counting the number of oscillations of a second oscillator on the FPGA during the predetermined time interval; and

generating a ratio between the resultant first and second oscillator counts that is used as the fingerprint.

Claims 9 – 11 (Cancelld)

12. (Currently Amended) A field programmable gate array (FPGA), comprising:

a plurality of configurable logic elements being programmable with configuration data to implement a desired circuit design;

a fingerprint element for generating a fingerprint representing inherent manufacturing process variations unique to the FPGA, wherein the fingerprint element includes a plurality of circuit elements, means for measuring propagation delays for each of the plurality of circuit elements and means for combining the propagation delays to generate the fingerprint; and

a decryption circuit coupled to receive encrypted configuration data, the decryption circuit configured to decrypt the encrypted configuration data using the fingerprint as a decryption key to extract the configuration data.

13. (Original) The FPGA of Claim 12, further comprising:

a configuration circuit for configuring the configurable logic elements with the configuration data.

Claim 14. (Cancelled)

15. (Currently Amended) The FPGA of Claim 12 [[14]], wherein the configuration data is encrypted using the fingerprint as an encryption key to generate the encrypted configuration data.

Claims 16-19 (Cancelled)

20. (Original) The FPGA of Claim 12, wherein the fingerprint element comprises:

an oscillator; and

a sensing circuit for counting the number of oscillations of the oscillator during a predetermined time interval.

21. (Original) The FPGA of Claim 20, wherein the oscillator comprises a configurable logic block.

22. (Original) The FPGA of Claim 12, wherein the fingerprint element comprises:

first and second oscillators; and

a sensing circuit, comprising:

means for counting the number of oscillations of the first and second oscillators during a predetermined time interval; and

means for generating a ratio between the resultant first and second binary oscillator count values, the ratio being used as the fingerprint.

Claims 23 – 43 (Cancelled)